UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/665,860	09/17/2003	John Alexander Bartas	P1437	8383

24739 7590 07/12/2006

CENTRAL COAST PATENT AGENCY
PO BOX 187
AROMAS, CA 95004

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 07/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/665,860	BARTAS, JOHN ALEXANDER	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 June 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13,15-22 and 24-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13,15-22 and 24-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Original application contained claims 1 – 55. Claim 1 has been amended in an amendment filed on 6/12/2006. The amendment filed have been entered and made of record. Presently, pending claims are 1 – 13, 15 – 22 and 24 – 32.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6/12/2006 has been entered.

Response to Argument

3. As per claim 1, Applicant asserts that Joiner never mentions hashing (Remarks: Page 9, 2nd Para). Examiner respectfully disagrees because Joiner teaches providing a network threat assessment method by comparing network data against the profiles such as virus signatures (Joiner: Column 3 Line 23 – 28 and Column 4 Line 48 – 53) and therefore, hashing must be used in conjunction with the manipulation of virus signatures. Applicant further asserts that: "the innovation is to avoid the recalculation of the hash value for each set of window-sized sequential bytes. Instead, we adjust the

hash value for the previous window by subtracting (or otherwise "un-hashing") the byte that is passing out of the window (byte 1 in the above example) and adding the value of the next byte entering the window (byte 10 in the above example)". Examiner notes Applicant's argument has no merit since the alleged limitation of subtracting and adding the values has not been recited into the claim. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1 – 10, 12, 15 – 22 and 24 – 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jacobson et al. (U.S. Patent 6044402), in view of Joiner (U.S. Patent 6742128), and in view of Caronni et al. (U.S. Patent 2002/0143850).

As per claim 1, Jacobson teaches a system for providing network security by managing and manipulating data connections and connection attempts initiated over a data-packet-network between at least two nodes connected to the network comprising:

a system host machine connected to the network; a first software application residing on the host machine for detecting and monitoring the live connections and connection attempts (Jacobson: Figure 1 & 8, Column 1 Line 66 – Column 2 Line 17 and Column 25 Line 8 – 18);

a data store for storing data about the connections and connection attempts (Jacobson: Figure 8 and Column 1 Line 66 – Column 2 Line 17); and

a second software application for emulating one or more end nodes of the connections or connection attempts (Jacobson: Column 2 Line 11 –Line 15 and Column 17 Line 10 – Line 67);

characterized in that the system using the detection software detects one or more pre-defined states associated with a particular connection or connection attempt in progress including those associated with any data content or type transferred and performs at least one packet generation and insertion action triggered by the detected state or states, the packet or packets emulating one or more end nodes of the connection or connection attempt to cause preemption or resolution of the detected state or states (Jacobson: Column 18 Line 60 – Column 19 Line 22).

Jacobson does not teach the hash routine utilizes at least one sliding window processing, in real time, the data passed over the live connection.

Joiner teaches the hash routine utilizes at least one sliding window processing, in real time, the data passed over the live connection (Joiner: Column 6 Line 10 – 17 and Column 8 Line 47 – 58: a data signature is managed by the hash routine and the

predetermined time period can be chosen to be a certain number of bytes duration that meets the Applicant's claimed language of "real time").

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Joiner within the system of Jacobson because (a) Jacobson teaches an intrusion detection system, and (b) Joiner teaches a more effective intrusion attempts detection method by assessing threats in use of profiles compared with the collected network data such as virus signature (Joiner: Column 3 Line 24 – 29).

Accordingly, Jacobson as modified teaches a third software application for detecting virus activity by hashing data passed over the live connection in real time and for comparing the hash data to a dataset containing virus signatures, the dataset searchable by hash table index, the hash entries therein derived individually from separate virus signatures. However, Jacobson as modified does not disclose expressly the dataset searchable by hash table index, the hash entries therein derived individually from separate virus signatures.

Caronni teaches the dataset searchable by hash table index, the hash entries therein derived individually from separate virus signatures (Caronni: Para [0029] Line 12 – 22).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Caronni within the system of Jacobson because (a) Jacobson teaches an intrusion detection system, and (b) Caronni teaches a more secure intrusion attempts detection method by assigning a dedicated-purpose

processing system to scan the data for the presence of any of the virus signature (Caronni: Para [0012] and Para [0029] Line 12 – 22).

As per claim 17, the claim limitations are met as the same reasons as that set forth above in rejecting claim 1 that contains all the limitations of claim 17.

As per claim 2 and 18, Jacobson as modified teaches the data-packet-network encompasses a Local Area Network connected to the Internet network enhanced with Transfer Control Protocol over Internet Protocol and User Datagram Protocol over Internet Protocol (Jacobson: Figure 2).

As per claim 3, Jacobson as modified teaches the system host machine is one of a desktop computer, a router, an embedded system, a laptop computer, or a server (Jacobson: Figure 4).

As per claim 4, Jacobson as modified teaches the system host is an especially dedicated piece of hardware (Jacobson: Figure 1 / Element 108).

As per claim 5 and 22, Jacobson as modified teaches emulation of the end nodes of the connections or connection attempts is performed by generation and insertion into a data stream of the connection or connection attempt data packets using Transfer Control Protocol over Internet Protocol, the packets emulating packets from the

current sending node in the connection (Jacobson: Column 18 Line 60 – Column 19 Line 22).

As per claim 6 and 21, Jacobson as modified teaches the packets inserted into a connection or connection attempt are one or a combination of Transfer Control Protocol reset packets or Transfer Control Protocol FIN packets (Jacobson: Column 18 Line 60 – Column 19 Line 22).

As per claim 7 and 24, Jacobson as modified teaches the nodes participating in the connections or connection attempts are desktop computers, servers, embedded systems, laptop computers or a combination thereof (Jacobson: Figure 1).

As per claim 8 and 19, Jacobson as modified teaches the data-packet-network is an Ethernet network connected to the Internet network and the first software application is an Ethernet driver set to operate in promiscuous mode (Jacobson: Column 4 Line 28).

As per claim 9, Jacobson as modified teaches the data about the connections or connection attempts includes one, more, or a combination of sender and receiver Internet Protocol addresses; Universal Resource Locators; source and destination ports; Transfer Control Protocol packet sequence numbers; Ethernet machine

addresses; domain names; and packet header details (Jacobson: Column 1 Line 66 – Column 2 Line 17).

As per claim 10, Jacobson as modified teaches the data store comprises segregated datasets representing one or more of banned Internet Protocol addresses; banned domain names; banned Universal Resource Locators; banned network ports; and virus signatures (Jacobson: Column 17 Line 60 – 67).

As per claim 12, Jacobson as modified teaches certain ones of the segregated datasets are built during runtime, maintained temporarily, and searchable by one of hash table indices or binary tree indices (Caronni: Para [0029] Line 12 – 22).

As per claim 15, Jacobson as modified teaches at least one sliding checksum window processes a data string from the data in the live connection in real time comprising a first hash value computed from a set number of consecutive bytes in the window, compared to the hash table index and stored, a second hash value is then computed and compared to the hash table index when the window slides to the next consecutive byte in the data string, wherein the second hash value equals the first hash value minus the byte existing the window plus the next consecutive byte of the data string entering the window, thereby creating a high speed search algorithm for the connection (Caronni: Para [0029] Line 12 – 22 & Joiner: Column 6 Line 10 – 17 and Column 8 Line 47 – 58: a data signature is managed by the hash routine and the

predetermined time period, as taught by Joiner, can be chosen to be as exactly one-byte time period duration that meets the Applicant's claimed language).

As per claim 16, Jacobson as modified teaches upon detecting a hit for a virus signature, the second software application interrupts data stream processing of one or more end points of the connection by sending a reset packet to stop download of the detected virus (Jacobson: Column 18 Line 60 – Column 19 Line 22).

As per claim 20, Jacobson as modified teaches manipulation of connection ends is performed by generation of and insertion of data packets to one or more nodes of the connection using Transfer Control Protocol over Internet Protocol, the generated packets emulating sender packets in construction and sequence number (Jacobson: Column 19 Line 12 – 21).

As per claim 25, Jacobson as modified teaches Transfer Control Protocol packets are generated and inserted according to pre-defined trigger events associated with existing states or knowledge of imminence thereof discovered during operation (Jacobson: Column 17 Line 16 – 65).

As per claim 26, Jacobson as modified teach including a third software application for detecting virus activity comprising: a software routine for hashing data passed over a formed data connection; and a software routine for comparing the hash

data to a dataset containing virus signatures, the dataset searchable by hash table index, the hash entries therein derived individually from separate virus signatures (Caronni: Para [0029] Line 12 – 22).

As per claim 27, Jacobson as modified teaches the predefined state is banned content and resolution thereof includes inserting content including machine readable script by one or a sequence of TCP packets containing replacement content (Jacobson: Column 19 Line 12 – 21).

As per claim 28, Jacobson as modified teaches virus searching is supported by algorithm supporting generation and then comparison of created hash values derived from active connection data streams to hash table entries stored in a data store and to return a hit upon obtaining a match (Joiner: Column 4 Line 48 – 53 and Column 6 Line 10 – 17 & Caronni: Para [0029] Line 12 – 22).

As per claim 29, Jacobson as modified teaches the third portion thereof is integrated with a messaging client for generating automated alerts to end nodes whose connections have been manipulated (Joiner: Column 8 Line 54 – 58).

As per claim 30, Jacobson as modified teaches including one or more sliding checksum windows for hashing data transferred over an active connection (Caronni: Para [0029] Line 12 – 22).

As per claim 31, Jacobson as modified teaches each checksum window processes 9 bytes of data 3-bytes at a time, each three-byte section treated as a single 24-bit number (Joiner: Column 8 Line 47 – 53: an obvious design choice).

5. Claims 11 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jacobson et al. (U.S. Patent 6044402), in view of Joiner (U.S. Patent 6742128), in view of Caronni et al. (U.S. Patent 2002/0143850), and in view of Vaidya (U.S. Patent 6279113).

As per claim 11, Jacobson as modified does not disclose expressly the data store further includes Ethernet machine addresses associated with bitmap icons representing individual machine types.

Vaidya teaches the data store further includes Ethernet machine addresses associated with bitmap icons representing individual machine types (Vaidya: Column 7 Line 19).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Vaidya within the system of Jacobson because (a) Jacobson teaches an intrusion detection system, and (b) Vaidya teaches a more effective intrusion attempts detection method by monitoring attack network address signatures (Vaidya: Column 1 Line 10 – 15).

As per claim 13, Jacobson does not disclose expressly certain ones of the segregated datasets are uploaded into host Random Access Memory upon booting of the host system.

Vaidya teaches certain ones of the segregated datasets are uploaded into host Random Access Memory upon booting of the host system (Vaidya: Column 5 Line 66).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Vaidya within the system of Jacobson because (a) Jacobson teaches an intrusion detection system, and (b) Vaidya teaches a more effective intrusion attempts detection method by monitoring attack network address signatures (Vaidya: Column 1 Line 10 – 15).

6. Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jacobson et al. (U.S. Patent 6044402), in view of Joiner (U.S. Patent 6742128), in view of Caronni et al. (U.S. Patent 2002/0143850), and in view of Weaver (U.S. Patent 6574669).

As per claim 32, Jacobson as modified does not disclose expressly the hash table is sparsely populated and wherein the hash table index thereof is bit-masked to reduce the overall size of the table and increase performance of the search.

Weaver teaches the hash table is sparsely populated and wherein the index thereof is bit-masked to reduce the overall size of the hash table table and increase performance of the search (Weaver: Figure 7C and Column 10 Line 1 – 9).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Weaver within the system of Jacobson as modified because (a) Jacobson teaches an intrusion detection processing system based on a pre-defined signature hash pattern in the network address block list, and (b) Weaver teaches a more effective hash processing system to optimize the search over a network address hash table (Weaver: Figure 7C and Column 10 Line 1 – 9).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100